A Tight Lower Bound for the BB84-states Quantum-Position-Verification Protocol

Jérémy Ribeiro and Frédéric Grosshans[*]

Laboratoire Aimé Cotton, CNRS,
Université Paris-Sud and ENS Cachan, F-91405 Orsay,
France

We use the entanglement sampling techniques developed in (Dupuis *et al.*, 2015) to find a lower bound on the entanglement needed by a coalition of cheater attacking the quantum postition verification protocol using the four BB84 states ($\texttt{QPV}_{\mathrm{BB84}}$) in the scenario where the cheaters have no access to a quantum channel but share a (possibly mixed) entangled state Φ. For a protocol using n qubits, a necessary condition for cheating is that the max- relative entropy of entanglement $E_{\max}(\Phi) \geq n - O(\log n)$. This improves previously known best lower bound by a factor ~ 4, and it is essentially tight, since it is vulnerable to a teleportation based attack using $n - O(1)$ ebits of entanglement.

Technical paper : arXiv:1504.07171

I. CONTEXT AND PREVIOUS WORK ON POSITION VERIFICATION CRYPTOGRAPHY

The very first (classical) position verification (PV) protocols have been distance bounding protocols, introduced in 1993 (Brands and Chaum, 1994) to prevent man-in-the-middle attacks. However, these protocols only work in some situations, and PV protocols by a coalition of distant verifiers $\{\mathsf{V}_i\}$ are more useful, as they allow to build localized authentication protocol, but also many other cryptographic applications, like key distribution at a specific place (Chandran *et al.*, 2009). However, (Chandran *et al.*, 2009) have shown that no classical PV protocol can be computationally secure against a coalition $\{\mathsf{M}_i\}$ of malicious provers.

Quantum position verification (QPV) protocols appeared the next year in the scientific literature, with publications of three independent teams (Buhrman *et al.*, 2014; Chandran *et al.*, 2010; Kent *et al.*, 2011, 2006; Malaney, 2010a,b). Even in the quantum case, unconditional security is unatainable (Buhrman *et al.*, 2014); a universal attack using an exponential amount of entanglement is known (Beigi and König, 2011). To guarantee the security of a QPV protocol one either needs a computational hypothesis (Unruh, 2014) or a bound on the quantum entanglement shared between the cheaters (Beigi and König, 2011; Buhrman *et al.*, 2014; Lau and Lo, 2011; Tomamichel *et al.*, 2013).

The present work is in the latter framework, where the cheating coalition $\{\mathsf{M}_i\}$ only has access to a limited amount of entanglement. Despite the exponential universal attack, the best lower bounds found so far have been linear (Beigi and König, 2011; Tomamichel *et al.*, 2013). To our knowledge, the protocol showing the best security in this framework is an expermentally impractical protocol, $\texttt{QPV}_{\mathrm{MUBs}}$, proposed in (Beigi and König, 2011): a n-qubits implementation of $\texttt{QPV}_{\mathrm{MUBs}}$ is secure against adversary holding less that $n/2$ ebits.

$\texttt{QPV}_{\mathrm{BB84}}$, introduced in (Buhrman *et al.*, 2014; Chandran *et al.*, 2010), is experimentally much simpler since it essentially uses quantum key distribution components, and (Tomamichel *et al.*, 2013) have proved its security against adversary holding less than $-\log_2(\cos^2(\pi/8)) \cdot n \simeq 0.22845 \cdot n$ ebits of entanglement. We improve this bound to $n - O(\log n)$ ebits. Since a teleportation-based explicit attack using $n - O(1)$ ebits is known (Kent *et al.*, 2011; Lau and Lo, 2011), this bound is tight.

Our argument is essentially that the winning conditions in $\texttt{QPV}_{\mathrm{BB84}}$, for a cheating coalition $\{\mathsf{M}_1, \mathsf{M}_2\}$, are essentially the same as the cheating condition of weak string erasure (WSE) in a variant of the noisy storage model (NSM), with supplementary conditions (M_1 also has to guess the string). $\texttt{QPV}_{\mathrm{BB84}}$ is therefore harder to defeat than WSE in the NSM, and we can adapt the security proof of WSE given in (Dupuis *et al.*, 2015) to our case.

II. MIN-ENTROPY AND MAX- RELATIVE ENTROPY OF ENTANGLEMENT

As usual in the security proof of such a quantum cryptographic procedure, the security is ensured by a lower bound on the conditonal min-entropy of entanglement $H_{\min}(X|B)$ where X is the classical bit-string to guess and B the (quantum and classical) information accessible to the cheater. This quantity is the logarithm of the winning probability of the cheater, a linearly increasing $H_{\min}$ corresponding to an exponentially decreasing cheating probability.

The relevant figure of merit of the bipartite quantum state Φ shared by the cheaters is the max- relative

[*] frederic.grosshans@u-psud.fr

entropy of entanglement $E_{\max}$, introduced by (Datta, 2009). This entanglement monotone is closely related to $H_{\min}$, and can be used to lower-bound it, since, for any bipartite system AB,

$$H_{\min}(A|B)_\rho \geq -E_{\max}(A;B)_\rho$$

III. WEAK STRING ERASURE AND ENTANGLEMENT SAMPLING

To cheat in a WSE in the NSM, Bob has to guess the n bits of X, with two informations :

- a noisy quantum memory B, wher he had previously stored quantum (and classical) information about of n-qubits encoding X in an unknown BB84 basis;
- The basis information Θ. He only learned Θ after the imperfections of the memory have taken effect.

(Dupuis *et al.*, 2015) use an entanglement sampling argument to bound $H_{\min}(X|\Theta B)$ by a monotonous function γ of $H_{\min}(A|\Theta B)$, the min-entropy in the equivalent entangled protocol, taken before Alice measures A to get X.

If we replace the quantum channel modeling the memory by a bipartite state, Φ, we are in a slightly different security model, the noisy entanglement model (NEM), but we can still use the same reasoning. We can also bound $H_{\min}(A|\Theta B)$ by $-E_{\max}(A;\Theta B)$ and use a monotony argument to bound the latter by $-E_{\max}(\Phi)$.

This allows us to show a lower bound on the entanglement needed to cheat for the WSE protocol with a probability at least ε.

$$E_{\max}(\Phi) \leq n - s - nh\left(\tfrac{s}{n}\right) \leq n - s\log_2 n + s\log_2 \tfrac{s}{2e}$$

where $s := 1 - 2\log_2$, e is the basis of the natural logarithm, and $h(\alpha) := -\alpha\log_2\alpha - (1-\alpha)\log_2(1-\alpha)$ is the binary entropy function.

IV. QUANTUM POSITION VERIFICATION SECURITY

To cheat in the (1D-)$\mathtt{QPV}_{\mathrm{BB84}}$ protocol, a coalition $\{\mathsf{M}_1, \mathsf{M}_2\}$ needs that both its members guess the same string X from different informations, with only 1 round of classical communication. If we only consider M_2's output, the problem is exactly the same as the WSE protocol in the NEM. In other words, if $\mathsf{M}_1, \mathsf{M}_2$ know a cheating strategy for $\mathtt{QPV}_{\mathrm{BB84}}$, they can use it with the same resources (*i.e.* the same state Φ) to cheat on WSE in the NEM. We can therefore directly transpose to $\mathtt{QPV}_{\mathrm{BB84}}$ the bound given above for WSE.

V. CONCLUSION

We have shown the security of the practical protocol $\mathtt{QPV}_{\mathrm{BB84}}$ in 1D against a coalition of cheaters sharing an entangled state of max- relative entropy of entanglement $E_{\max}(\Phi) \leq n - O(\log n)$. This bound is the best known to date for a QPV protocol and is essentially tight for $\mathtt{QPV}_{\mathrm{BB84}}$, since an attack using $n - O(1)$ ebits is known.

REFERENCES

Beigi, S., and R. König (2011), New Journal of Physics **13**, 093036, arXiv:1101.1065.

Brands, S., and D. Chaum (1994), in *Advances in Cryptology — EUROCRYPT '93*, Lecture Notes in Computer Science, Vol. 765, edited by T. Helleseth (Springer Berlin Heidelberg) pp. 344–359.

Buhrman, H., N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner (2014), SIAM Journal on Computing **43** (1), 150, 1009.2490.

Chandran, N., S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky (2010), Withdrawn and replaced by (Buhrman *et al.*, 2014), arXiv:1005.1750v1.

Chandran, N., V. Goyal, R. Moriarty, and R. Ostrovsky (2009), in *Advances in Cryptology - CRYPTO 2009*, Lecture Notes in Computer Science, Vol. 5677, edited by S. Halevi (Springer Berlin Heidelberg) pp. 391–407, IACR:2009/364.

Datta, N. (2009), Information Theory, IEEE Transactions on **55** (6), 2816, arXiv:0803.2770.

Dupuis, F., O. Fawzi, and S. Wehner (2015), IEEE Transactions on Information Theory **61** (2), 1093, arXiv:1305.1316.

Kent, A., W. J. Munro, and T. P. Spiller (2011), Phys. Rev. A **84**, 012326, arXiv:1008.2147.

Kent, A. P., W. J. Munro, T. P. Spiller, and R. G. Beausoleil (2006), "Quantum tagging," US patent 7,075,438.

Lau, H.-K., and H.-K. Lo (2011), Phys. Rev. A **83**, 012322, arXiv:1009.2256.

Malaney, R. A. (2010a), Phys. Rev. A **81**, 042319, arXiv:1003.0949.

Malaney, R. A. (2010b), in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1–6, arXiv:1004.4689.

Tomamichel, M., S. Fehr, J. Kaniewski, and S. Wehner (2013), New Journal of Physics **15**, 103002, arXiv:1210.4359.

Unruh, D. (2014), in *Advances in Cryptology – CRYPTO 2014*, Lecture Notes in Computer Science, Vol. 8617, edited by J. A. Garay and R. Gennaro (Springer Berlin Heidelberg) pp. 1–18, IACR:2014/118.